On quantitative analogues of the Goldbach and twin prime conjectures over $\mathbf{F}_q[t]$

Andreas O. Bender
School of Mathematics
Korea Institute for Advanced Study
Seoul 130-722
Republic of Korea
andreas@kias.re.kr

Paul Pollack*
School of Mathematics
Institute for Advanced Study
Einstein Drive
Princeton, NJ 08540, USA
pppollac@illinois.edu

September 8th, 2009

Abstract

We study the number of ways to decompose a monic $F \in \mathbf{F}_q[t]$ of degree n as a sum of two monic irreducible polynomials in $\mathbf{F}_q[t]$. Our principal result is an asymptotic formula for the number of such representations in the case when q is large compared to n. In its range of validity, this formula agrees with what is suggested by heuristic arguments from the rational setting. We also present similar results towards an analogue of the twin prime conjecture.

Mathematics subject classification (2000): 11T55, 11N32.

1   Introduction

In this article we consider analogues of the Goldbach and twin prime conjectures in the setting of polynomials over finite fields. Both conjectures then become two-parameter problems, with one parameter the size q of the finite field and the other the degree of the polynomial. We prove that every polynomial of a given degree n has as many representations as a sum of two irreducible polynomials

---

as heuristic arguments lead one to expect, provided that q is odd and large in comparison to n. We also show, under similar restrictions on q and n, that the number of twin prime pairs of a given degree n is as expected. Our results leave open the seemingly very hard question of what happens over a fixed finite field $\mathbf{F}_q$.

Define a *Goldbach representation* of F to be a way of writing F in the form $F_1 + F_2$, where F_1 and F_2 are monic irreducible polynomials in $\mathbf{F}_q[t]$ with $\deg F_1 = \deg F - 1$ and $\deg F_2 = \deg F$.[1] We write $R(F; q)$ for the number of Goldbach representations of F. It is easy to formulate a guess as to how large $R(F; q)$ should be; heuristic arguments which are familiar from the theory of rational primes (see, e.g., [4, §1.2.3]) suggest that for a monic polynomial F of degree n, we should have

$$R(F; q) \approx \frac{q^{n-1}}{n(n-1)} \prod_{P|F} \left(1 - \frac{1}{|P|}\right)^{-1} \prod_{P \nmid F} \left(1 - \frac{1}{(|P|-1)^2}\right) \tag{1}$$

for a wide range of parameters.[2] In fact, it is plausible to conjecture that the left and right-hand sides in the formula above are asymptotic to one another in any range of the q and n space where $q^n \to \infty$ and $n \geq 3$, uniformly in F. (We include the restriction $n \geq 3$ because in characteristic 2, polynomials of the form $T^2 + T + \alpha$ do not have a Goldbach representation.) A similar conjecture was proposed by the second author as Conjecture 7.1.1 in [9].

It seems very difficult to prove anything in the direction of (1) when working over a fixed finite field $\mathbf{F}_q$. However, the situation improves if we allow q to vary. The following two theorems are due to the first author (see [1, 2], and cf. [9, Chapter 7]):

Theorem A. *Let $\mathbf{F}_q$ be a fixed finite field of odd cardinality q, and let F be a monic polynomial in $\mathbf{F}_q[t]$ of degree $n \geq 2$. If s is sufficiently large, then F has a Goldbach representation in $\mathbf{F}_{q^s}[t]$.*

Theorem B. *Let $\mathbf{F}_q$ be a finite field of odd cardinality q, and let F be a monic polynomial in $\mathbf{F}_q[t]$ of degree $n \geq 2$. If $q > 8(n+6)^{2n^2}$, then F has a Goldbach representation in $\mathbf{F}_q[t]$.*

Our first result is that if q is large compared to n, then $R(F; q)$ is precisely as large as predicted by (1).

Theorem 1.1. *Let $\mathbf{F}_q$ be a finite field of odd order q. Suppose that $F \in \mathbf{F}_q[t]$ is a monic polynomial of degree $n \geq 2$. Then*

$$R(F; q) = \frac{q^{n-1}}{n(n-1)} + O(n!(n-1)!q^{n-3/2}) + O(n \cdot 2^{\binom{n+2}{2}} q^{n-2}),$$

where the implied constants are absolute.

---

[1]Rather than prescribing that $\deg F_1 = \deg F - 1$, one could permit any F_1 with $\deg F_1 < \deg F$, which is how the ternary Goldbach problem is handled in [5]. However, in the range of q and n of interest to us, that choice turns out to affect neither the conjectured asymptotic (1) for the number of Goldbach representations nor the statement of our Theorem 1.1.

[2]Here we write $|A|$ for $q^{\deg A}$, so that $|A| = \#\mathbf{F}_q[T]/(A)$ for each nonzero polynomial A.

After a short computation, one obtains from Theorem 1.1 that for odd q,

$$R(F; q) \sim \frac{q^{n-1}}{n(n-1)} \quad \text{whenever} \quad \frac{q}{n^3 2^{\binom{n+2}{2}}} \to \infty. \tag{2}$$

It may not be immediately obvious that this asymptotic agrees with our prediction (1), since the two products in (1) are absent in (2), but in our range of q and n, both of these products are easily verified to be tending towards 1.

We can prove similar results towards a polynomial version of the twin prime conjecture. Let A be a polynomial in $\mathbf{F}_q[t]$. Barring congruence obstructions, one expects that there are infinitely many monic polynomials $F \in \mathbf{F}_q[t]$ for which both F and $F + A$ are irreducible. If A is a constant polynomial, this can be proved by a method of C. Hall (see [7, Theorem 1.2]), but it seems very difficult to confirm this prediction for other values of A.

If $A \in \mathbf{F}_q[t]$ and $\deg A < n$, we write $\pi_2(n; A, q)$ for the number of monic polynomials F of degree n for which both F and $F + A$ are irreducible. Here heuristics suggest (cf. [8, Conjecture 1]) that

$$\pi_2(n; A, q) \approx \frac{q^n}{n^2} \prod_{P|A} \left(1 - \frac{1}{|P|}\right)^{-1} \prod_{P \nmid A} \left(1 - \frac{1}{(|P| - 1)^2}\right). \tag{3}$$

We prove the following two results:

Theorem 1.2. *Let $\mathbf{F}_q$ be a finite field of odd cardinality q. Let n be a natural number, and let A be a nonzero polynomial in $\mathbf{F}_q[t]$ of degree smaller than n. If s is sufficiently large, then one can always find a monic polynomial $P \in \mathbf{F}_{q^s}[t]$ of degree n for which both P and $P + A$ are irreducible over $\mathbf{F}_{q^s}$.*

Theorem 1.3. *Let $\mathbf{F}_q$ be a finite field of odd cardinality q. Let n be a natural number, and let A be a nonzero polynomial in $\mathbf{F}_q[t]$ of degree smaller than n. Then*

$$\pi_2(n; A, q) = \frac{q^n}{n^2} + O(n!^2 q^{n-1/2}) + O(n \cdot 2^{\binom{n+2}{2}} q^{n-1}),$$

where the implied constants are absolute.

Of course Theorem 1.2 is contained in Theorem 1.3, but the strategy of proof suggests to prove the two results separately. Theorem 1.3 gives us an asymptotic formula for $\pi_2(n; A, q)$ in the range of q and n indicated in (2), and this formula agrees with the prediction (3) in this range of q vs. n.

A version of Theorem 1.3 appeared in the second author's Ph. D. thesis [9, Theorem 7.1.4] under a sharper restriction on the characteristic of $\mathbf{F}_q$.

Notation

We write p for the characteristic of $\mathbf{F}_q$ and use $\mathbf{F}$ for a fixed algebraic closure.

2 The polynomial Goldbach problem

Proof of Theorem 1.1

For certain details we shall refer the reader to [2]. Let $\mathcal{F}$ be the set of polynomials $f(x,t) \in \mathbf{F}_q[x,t]$ of total degree $n-1$ for which $f(t+b,t)$ is a monic, degree $n-1$ polynomial in t for every choice of $b \in \mathbf{F}_q$. Then (see [2, p. 7]) we have $\#\mathcal{F} = q^I$, where $I := \binom{n+1}{2} - 1$.

For every monic polynomial $g \in \mathbf{F}_q[t]$ of degree $n-1$, let N_g be the number of ordered pairs $(f(x,t), b)$ with $f(t+b,t) = g$, where $f \in \mathcal{F}$ and $b \in \mathbf{F}_q$. Then we have the following simple observation.

Lemma 2.1. *For every monic polynomial $g \in \mathbf{F}_q[t]$ of degree $n-1$, we have*

$$N_g = q^{\binom{n+1}{2} - (n-1)} = q^{I-n+2}.$$

Proof. Let $b \in \mathbf{F}_q$. Suppose $c_1(x), \ldots, c_{n-1}(x) \in \mathbf{F}_q[x]$ and that the degree of each c_i does not exceed $n-1-i$. Then there is a unique choice of $c_0(x) \in \mathbf{F}_q[x]$ for which $f(x,t) := \sum_{i=0}^{n-1} c_i(x) t^i$ belongs to $\mathcal{F}$ and satisfies $f(t+b,t) = g(t)$, namely

$$c_0(x) := g(x-b) - \sum_{i=1}^{n-1} c_i(x)(x-b)^i.$$

It follows that

$$N_g = q \cdot q^{1+2+\cdots+(n-1)} = q^{n(n-1)/2+1} = q^{n(n+1)/2-(n-1)},$$

as desired. $\qquad\square$

Let F be a univariate polynomial of degree $n \geq 2$ over $\mathbf{F}_q$, and let $\mathcal{R}$ be the set of degree $n-1$ Goldbach summands of F, i.e.,

$$\mathcal{R} := \{g \in \mathbf{F}_q[t] : \deg g = n-1, \text{ both } g \text{ and } F-g \text{ are monic irreducibles}\}.$$

Thus $R(F;q) = \#\mathcal{R}$. Lemma 2.1 reduces Theorem 1.1 to the following estimate for $\sum_{g \in \mathcal{R}} N_g$.

Lemma 2.2. *We have*

$$\sum_{g \in \mathcal{R}} N_g = \frac{q^{I+1}}{n(n-1)} + O(Nq^{I+1/2}) + O(q^I 2^{\binom{n+2}{2}} n),$$

where $N := (n-1)!n!$.

The proof of Lemma 2.2 depends on the following lemma due to Fried & Jarden ([6, Proposition 6.4.8]).

Lemma 2.3 (Explicit Chebotarev density theorem for degree 1 primes)**.** *Suppose that $L/\mathbf{F}_q(u)$ be a finite, geometric Galois extension of degree N. Let $\mathcal{C}$ be a conjugacy class of $\mathrm{Gal}(L/\mathbf{F}_q(u))$ and let $\mathcal{P}$ be the set of unramified, degree 1 primes of $\mathbf{F}_q(u)$ for which $\left(\frac{L/\mathbf{F}_q(u)}{P}\right) = \mathcal{C}$. Then, with g denoting the genus of $L/\mathbf{F}_q$, we have*

$$\left| \#\mathcal{P} - \frac{\#\mathcal{C}}{N} q \right| \leq 2 \frac{\#\mathcal{C}}{N}(g q^{1/2} + g + N).$$

Note that the estimate differs from Proposition 6.4.8 in [6] since, in their notation, we have $k = 1$ and therefore the second term in the first formula on page 120 is just the empty set.

We also require the following lemma ([9, Lemma 4.3.2]; see also [3, §3]).

Lemma 2.4. *Let $f(t, u) \in \mathbf{F}_q[t, u]$. Suppose that f as a polynomial in t is monic of degree n and is irreducible and separable over $\mathbf{F}_q(u)$. Let K be the splitting field of f over $\mathbf{F}_q(u)$. Suppose that for the element $b \in \mathbf{F}_q$, the discriminant of the polynomial $f(t, b)$ is nonzero. Then $f(t, b)$ is irreducible over $\mathbf{F}_q$ precisely when the Frobenius conjugacy class $(K/\mathbf{F}_q(u), P_b)$ is the conjugacy class of an n-cycle in $\mathrm{Gal}(K/\mathbf{F}_q(u))$. Here P_b denotes the prime of $\mathbf{F}_q(u)$ associated to the $(u - b)$-adic valuation.*

Remark. Suppose that $\deg_u f = m$. Then the t-discriminant of $f(t, u)$ is a polynomial in u of degree not exceeding $(2n - 1)m$, as one sees by applying the Sylvester determinant representation of the discriminant. Moreover, this t-discriminant is nonvanishing, since f is separable by hypothesis. Therefore the hypothesis of the lemma excludes at most $(2n - 1)m$ values of $b \in \mathbf{F}_q$.

Proof of Lemma 2.2. Recalling the definition of N_g, we find that

$$\sum_{g \in \mathcal{R}} N_g = \sum_{f \in \mathcal{F}} \quad \sum_{\substack{b \in \mathbf{F}_q \\ f(t+b,t) \text{ and } F-f(t+b,t) \text{ both irreducible}}} 1. \qquad (4)$$

We shall show that when q is large compared to n, the inner sum can be estimated fairly precisely for almost all choices of $f \in \mathcal{F}$.

Indeed, in [2] it is shown that for q large compared to n, most $f \in \mathcal{F}$ are such that both of the following statements hold:

- Let K_1 be the splitting field of $f(t + u, t)$ over $\mathbf{F}_q(u)$ and let K_2 be the splitting field of $F(t) - f(t + u, t)$ over $\mathbf{F}_q(u)$. Then $\mathrm{Gal}(K_1/\mathbf{F}_q(u))$ is the full symmetric group on $n - 1$ letters and $\mathrm{Gal}(K_2/\mathbf{F}_q(u))$ is the full symmetric group on n letters.

- Let L be the compositum of K_1 and K_2. Then $L/\mathbf{F}_q(u)$ is a geometric Galois extension, and the map

$$\mathrm{Gal}(L/\mathbf{F}_q(u)) \cong \mathrm{Gal}(K_1/\mathbf{F}_q(u)) \times \mathrm{Gal}(K_2/\mathbf{F}_q(u)), \qquad (5)$$
$$\sigma \mapsto (\sigma|_{K_1}, \sigma|_{K_2})$$

  is an isomorphism.

More precisely, this holds for all $f \in \mathcal{F}$ satisfying seven technical conditions ([2, p. 4], cf. the six conditions of §3 below), which in total exclude

$$\ll n \cdot 2^{\binom{n+2}{2}} q^{I-1} \tag{6}$$

polynomials $f \in \mathcal{F}$ (see [2, p. 8]). Let $\mathcal{F}'$ be the subset of $\mathcal{F}$ consisting of nonexceptional polynomials, so that (6) is an upper bound on $\#\mathcal{F} \setminus \mathcal{F}'$.

Suppose $f \in \mathcal{F}'$. By Lemma 2.4 and the subsequent remark, we have that excluding $O(n^2)$ values of $b \in \mathbf{F}_q$, the polynomial $f(t+b,t)$ is irreducible precisely when $(K_1/\mathbf{F}_q(u), P_b)$ is the conjugacy class of an $(n-1)$-cycle. Similarly, excluding $O(n^2)$ values of b, we have that $F - f(t+b,t)$ is irreducible exactly when $(K_2/\mathbf{F}_q(u), P_b)$ is the conjugacy class of an n-cycle. This means that by (5), the simultaneous irreducibility of these polynomials is, excepting $O(n^2)$ values of b, equivalent to $(L/\mathbf{F}_q(u), P_b)$ belonging to a certain conjugacy class $\mathcal{C}$ of $\mathrm{Gal}(L/\mathbf{F}_q(u))$ of order $(n-2)!(n-1)!$.

We apply the version of the Chebotarev density theorem quoted above with this conjugacy class $\mathcal{C}$. Since $[L : \mathbf{F}_q(u)] = (n-1)!n! = N$, we find that for $f \in \mathcal{F}'$, the inner sum in (4) is

$$\frac{q}{n(n-1)} + O\left(\frac{1}{n^2}(gq^{1/2} + g + N)\right) + O(n^2).$$

It can be shown that $g = 1 + N(n^2 - 2n)$ (see [2, p. 9]), which implies a bound on the error terms of $O(Nq^{1/2})$. Summing over $\mathcal{F} = \mathcal{F}' \cup (\mathcal{F} \setminus \mathcal{F}')$, we find that the sum in (4) is given by

$$\sum_{f \in \mathcal{F}'} \frac{q}{n(n-1)} + O(\#\mathcal{F}' N q^{1/2}) + O(q(\#\mathcal{F} \setminus \mathcal{F}'))$$

$$= \frac{q^{I+1}}{n(n-1)} + O\left(\frac{q}{n(n-1)} \#\mathcal{F} \setminus \mathcal{F}'\right) + O(Nq^{I+1/2}) + O(q\#\mathcal{F} \setminus \mathcal{F}')$$

$$= \frac{q^{I+1}}{n(n-1)} + O(Nq^{I+1/2}) + O(n \cdot 2^{\binom{n+2}{2}} q^I),$$

using the trivial estimate $\#\mathcal{F}' \leq \#\mathcal{F} = q^I$ and the bound (6) for $\#\mathcal{F} \setminus \mathcal{F}'$. $\quad\square$

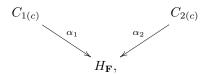## 3   The polynomial twin prime problem

Proof of Theorem 1.2

The proof is very similar to that of Theorem A given in [2]. Let $\mathfrak{X}$ denote the family of all plane algebraic curves $f_{1(c)}(x,t) = 0$ over $\mathbf{F}$ of degree at most n in $\mathbf{A}^2$. Let $I = \binom{n+2}{2} - 1$ and fix an embedding of $\mathfrak{X}$ by a map

$$\begin{aligned}
\mathfrak{X} &\longrightarrow \mathbf{A}^{I+1} \times \mathbf{A}^2, \\
f_{1(c)} &\mapsto (c) \times \{f_{1(c)}(x,t) = 0\},
\end{aligned}$$

where (c) is the coefficient vector of $f_{1(c)}$. Let $\mathcal{F}$ be the family of affine curves of degree n in $\mathbf{A}^2$ such that $f_{1(c)}(t+b, t)$ is monic for any b. The coefficients (c) of such a curve correspond to a point on an affine subspace $H \subset \mathbf{A}^{I+1}$ of codimension one. In particular, we have that $\#\mathcal{F} = q^I$. For any element $f_{1(c)} \in \mathcal{F}$ with coordinates $(c) \in H_{\mathbf{F}}$, we set

$$f_{2(c)}(x, t) = f_{1(c)}(x, t) + A(t).$$

We consider the families of curves in $H_{\mathbf{F}} \times \mathbf{P}_{\mathbf{F}}^2$

$$
\begin{array}{ccc}
C_{1(c)} & & C_{2(c)} \\
& \searrow^{\alpha_1} \quad \swarrow^{\alpha_2} & \\
& H_{\mathbf{F}}, &
\end{array}
$$

where $C_{i(c)} = \alpha_i^{-1}(c)$ denotes the Zariski closure of the affine curve $f_{i(c)}(x, t) = 0$ in $\mathbf{P}_{\mathbf{F}}^2$. Let β_i denote the rational map $C_i \to \mathbf{P}^1$ given by the projection from $M = (1, 1, 0)$ in homogenised coordinates (x, t, z). The maps β_1 and β_2 are in fact morphisms since the point M does not lie on $C_{1(c)}$ or $C_{2(c)}$. Indeed, we are assuming $(c) \in H$ and so monicity of the two polynomials $f_i(t+b, t)$ for any b implies that $M \notin C_i$.

Imitating the argument of [2], we prove the following: For all sufficiently large s, there is a point (c) in $H_{\mathbf{F}_{q^s}}(\mathbf{F}_{q^s})$ such that the following conditions are satisfied:

1. Both $C_{1(c)}$ and $C_{2(c)}$ are smooth.

2. Both $C_{1(c)}$ and $C_{2(c)}$ are absolutely irreducible.

3. The Gauss maps of both $C_{1(c)}$ and $C_{2(c)}$ are separable.

4. The morphisms β_1 and β_2 are generic (in the sense of [2, Definition 2.2]).

5. No line $x = t + b$ is tangent to both $C_{1(c)}$ and $C_{2(c)}$.

6. The line at infinity is not tangent to C_1 or C_2.

For each of the six conditions, the points (c) satisfying it form an open subscheme of $H_{\mathbf{F}}$. We now check that each of these subschemes is nonempty.

For the smoothness condition (1), we consider two cases: First suppose that $p \nmid n$. Consider the polynomial $f_1 := 2x^n - t^n + d$, where $d \in \mathbf{F}_q$. A short calculation shows that $C_{1(c)}$ is smooth for any nonzero d, while $C_{2(c)}$ is singular for at most n different values of d. So suppose that p divides n, and write

$$A(t) = a_m t^m + a_{m-1} t^{m-1} + \cdots + a_1 t + a_0.$$

Consider

$$f_1 := 2x^n + x - t^n + dt^{n-1}.$$

If $d \neq 0$ it is easily checked that $C_{1(c)}$ is smooth. The nonvanishing of d also guarantees that $C_{2(c)}$ is smooth, unless $m = n - 1$, in which case smoothness follows under the additional assumption that $d + a_m \neq 0$. Therefore in either case the points $(c) \in H$ whose fibres $C_{i(c)}$ are smooth curves form a nonempty open subscheme A_1 (say).

To show that the subscheme A_2 corresponding to condition (2) is nonempty, we have to exhibit an $f_{1(c)}$ with $(c) \in H$ for which both $f_{1(c)}$ and $f_{2(c)} := f_{1(c)} + A(t)$ are absolutely irreducible. Consider

$$f_1 := x^n + b_1 t + b_0,$$

where b_0 and b_1 are chosen so that $b_1 \neq 0$, $b_1 \neq -a_1$ and $b_0 = -a_0$. Then the Eisenstein criterion implies the absolute irreducibility of both $f_{1(c)}$ and $f_{1(c)} + A(t)$, the respective primes being $b_1 t + b_0$ and t.

Now consider the condition (3) of separability of the Gauss maps. This corresponds to the subscheme A_3, for which we consider

$$f_1 := 2x^n - x^2 t^{n-2}.$$

It follows that A_3 is nonempty since both $f_1(c)$ and $f_2(c)$ intersect the line at infinity in a point of multiplicity 2.

Conditions (4)–(6) can be treated by the same argument used to treat conditions (4)–(7) in [2, bottom of p.5]. The single change necessary is that we now require an example showing the nonemptiness of the open subscheme corresponding to the values (c) for which the line at infinity is tangent to neither $C_{1(c)}$ nor $C_{2(c)}$. We may choose

$$f_1 := 2x^{n-j} t^j - t^n$$

with $j = 1$ if $p \mid n$ and $j = 0$ otherwise.

To complete the proof of Theorem 1.2 it is enough to apply the Chebotarev density theorem exactly as in the corresponding proof of Theorem A. We obtain that for s sufficiently large, there is a $b_0 \in \mathbf{F}_{q^s}$ for which both $f_1(t + b_0, t)$ and $f_2(t + b_0, t) = f_1(t + b_0, t) + A(t)$ are irreducible. This means that $f_1(t + b_0, t)$ and $f_2(t + b_0, t)$ are our desired twin prime pair.

Proof of Theorem 1.3

With the proof of Theorem 1.2 out of the way, we can prove Theorem 1.3 by an argument analogous to that given for Theorem 1.1 above. Setting

$$\mathcal{T} := \{g \in \mathbf{F}_q[t] : \deg g = n, \text{ both } g \text{ and } g + A \text{ are monic irreducibles}\},$$

we have $\pi_2(n; A, q) = \#\mathcal{T}$. As in §2, let N_g be the number of pairs $(f(x, t), b)$ with $f \in \mathcal{F}$, $b \in \mathbf{F}_q$, and $f(t + b, t) = g$. Since now the polynomials $f \in \mathcal{F}$ have total degree n, we replace $n - 1$ by n in Lemma 2.1 to obtain the following.

Lemma 3.1. *For every monic polynomial $g \in \mathbf{F}_q[t]$ of degree n, we have $N_g = q^{\binom{n+2}{2}-n} = q^{I+1-n}$.*

To estimate the inner sum of

$$\sum_{g \in \mathcal{T}} N_g = \sum_{f \in \mathcal{F}} \sum_{\substack{b \in \mathbf{F}_q \\ f(t+b,t) \text{ and } f(t+b,t)+A(t) \text{ both irreducible}}} 1, \qquad (7)$$

we observe that a calculation almost identical to the one appearing in [2, §3] shows that conditions (1)–(6) above are satisfied for all $f \in \mathcal{F}$ with $\ll n \cdot 2^{\binom{n+2}{2}} q^{I-1}$ exceptions. Let $\mathcal{F}'$ be the set of nonexceptional $f \in \mathcal{F}$. Then for each $f \in \mathcal{F}'$ both the following statements hold.

1. Let K_1 be the splitting field of $f(t + u, t)$ over $\mathbf{F}_q(u)$ and let K_2 be the splitting field of $f(t + u, t) + A(t)$ over $\mathbf{F}_q(u)$. Then $\mathrm{Gal}(K_1/\mathbf{F}_q(u))$ and $\mathrm{Gal}(K_2/\mathbf{F}_q(u))$ are both the full symmetric group on n letters.

2. Let L be the compositum of K_1 and K_2. Then $L/\mathbf{F}_q(u)$ is a geometric Galois extension and the map

$$\mathrm{Gal}(L/\mathbf{F}_q(u)) \cong \mathrm{Gal}(K_1/\mathbf{F}_q(u)) \times \mathrm{Gal}(K_2/\mathbf{F}_q(u)),$$
$$\sigma \mapsto (\sigma|_{K_1}, \sigma|_{K_2})$$

   is an isomorphism.

Proceeding as in the proof of Theorem 1.1, we obtain from Lemma 2.3 that for each $f \in \mathcal{F}'$ the inner sum in (7) is

$$\frac{q}{n^2} + O\left(\frac{1}{n^2}(gq^{1/2} + g + N)\right) + O(n^2). \qquad (8)$$

Here $N = [L : \mathbf{F}_q(u)] = n!^2$ and g is the genus of L over $\mathbf{F}_q$. By formula (4) of [3] and the well-known formula for the genus of an irreducible smooth plane algebraic curve, we find after a short calculation that

$$g = 1 + N(n^2 - n - 1).$$

This shows that the O-terms in (8) are $O(Nq^{1/2})$. Now following the proof in §2, we find that the double sum on the right-hand side of (7) is

$$\frac{q^{I+1}}{n^2} + O\left(Nq^{I+1/2}\right) + O\left(n \cdot 2^{\binom{n+2}{2}} q^I\right).$$

But from Lemma 3.1, this double sum is precisely $q^{I+1-n} \# \mathcal{T}$. Theorem 1.3 follows.

9

References

[1] A. O. Bender, *Decompositions into sums of two irreducibles in* $\mathbf{F}_q[t]$, C. R. Math. Acad. Sci. Paris **346** (2008), no. 17-18, 931–934.

[2] ———, *Representing an element in* $\mathbf{F}_q[t]$ *as the sum of two irreducibles in* $\mathbf{F}_{q^s}[t]$, arXiv:0809.4381v1 [math.NT], 2008.

[3] A. O. Bender and O. Wittenberg, *A potential analogue of Schinzel's hypothesis for polynomials with coefficients in* $\mathbb{F}_q[t]$, Int. Math. Res. Not. (2005), no. 36, 2237–2248.

[4] R. Crandall and C. Pomerance, *Prime numbers: A computational perspective*, second ed., Springer, New York, 2005.

[5] G. W. Effinger and D. R. Hayes, *Additive number theory of polynomials over a finite field*, Oxford Mathematical Monographs, The Clarendon Press Oxford University Press, New York, 1991, Oxford Science Publications.

[6] M. D. Fried and M. Jarden, *Field arithmetic*, second ed., Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics], vol. 11, Springer-Verlag, Berlin, 2005.

[7] P. Pollack, *An explicit approach to hypothesis H for polynomials over a finite field*, Anatomy of integers, CRM Proc. Lecture Notes, vol. 46, Amer. Math. Soc., Providence, RI, 2008, pp. 259–273.

[8] ———, *A polynomial analogue of the twin prime conjecture*, Proc. Amer. Math. Soc. **136** (2008), no. 11, 3775–3784. MR MR2425715

[9] ———, *Prime polynomials over finite fields*, Ph.D. thesis, Dartmouth College, 2008.